BEST AVAILABLE COPY

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number
WO 2004/088641 A2

(51) International Patent Classification[7]: G11B

(21) International Application Number:
PCT/US2004/009149

(22) International Filing Date: 25 March 2004 (25.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/457,716	26 March 2003 (26.03.2003)	US
Not furnished	25 March 2004 (25.03.2004)	US

(71) Applicant *(for all designated States except US)*: **WAY SYSTEMS, INC.** [US/US]; 200 Unicorn Park, Woburn, MA 01801 (US).

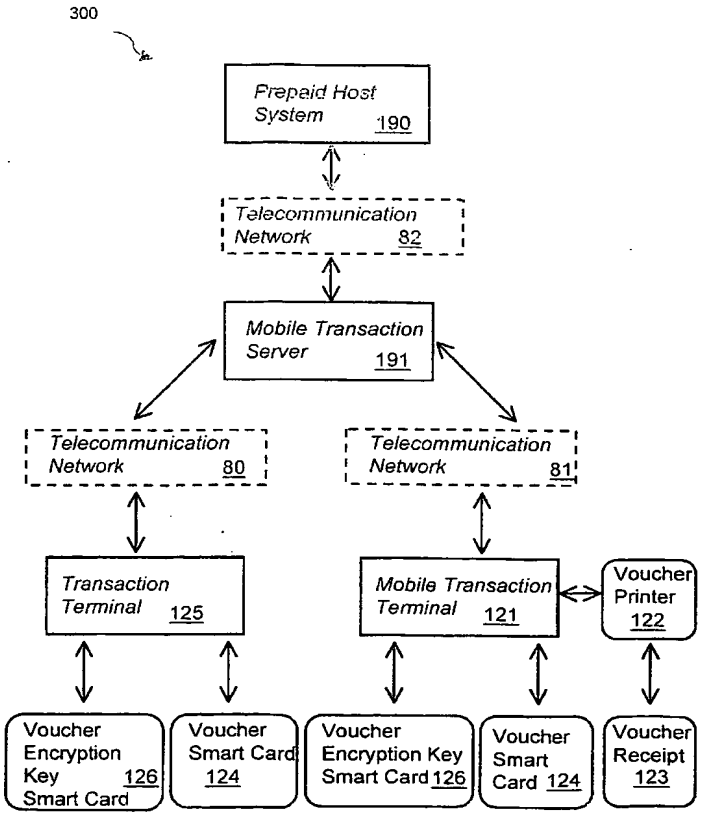
(71) Applicants and
(72) Inventors: **GOLDTHWAITE, Scott** [US/US]; 15 Oregon Court, Hingham, MA 02043 (US). **BALSAN, Damien** [US/US]; 78 Melrose Street, Arlington, MA 02474 (US).

(74) Agent: **COLLINS, Aliki, K.. ph. d.**; AKC Patents, 215 Grove Street, Newton, MA 02466 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS



(57) Abstract: The present invention describes a system and a method that utilizes transaction terminals (125, 121) equipped with smart card readers to download and store a batch of multiple prepaid electronic vouchers to a smart card (124), retrieve and decrypt individual prepaid vouchers from the smart card and print a voucher receipt with a printer (122) in connection with the transaction terminal. The transaction terminals (125, 121) are in connection with a mobile transaction server (191) that acts as a gateway to a prepaid system (190) and routes transactions between transaction terminals and the prepaid system and between transaction terminals. The present invention also describes a method for storing a voucher encryption key on a second smart card or hardware security module. The voucher encryption key is utilized to decrypt encrypted vouchers on a voucher repository smart card. The present invention also describes a method of transferring encrypted vouchers between voucher smart cards using a single transaction terminal or multiple transaction terminals. The transaction terminals may be mobile devices communicating to the mobile transaction server over wireless networks or computers connected to a wired network.

WO 2004/088641 A2

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS

Cross Reference to related Co-Pending Applications

This application claims the benefit of U.S. provisional application Serial No. 60/457,716 filed on March 26, 2003 and entitled SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS, which is commonly assigned and the contents of which are expressly incorporated herein by reference.

This application is also a continuation in part of U.S. applications Serial No. 10/205,768, 10/625,823, and 10/695,585, filed on July 26, 2002, July 23, 2003, and October 28, 2003, and entitled "SYSTEM AND METHOD FOR PAYMENT TRANSACTION AUTHENTICATION", "MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER/WRITER", and "MOBILE COMMUNICATION DEVICE EQUIPPED WITH A MAGNETIC STRIPE READER", respectively, the contents of which applications are expressly incorporated herein by reference.

Field of the Invention

The present invention relates to a system and a method for securely storing prepaid top up vouchers on a smart card and utilizing mobile devices to generate the vouchers at the time of purchase.

Background of the Invention

The market for mobile/wireless phone usage has rapidly expanded to reach over 1 billion subscribers throughout the world by the end of 2002. Over 60% of these subscribers prepay for mobile phone usage. The greatest growth of mobile phone subscribers occurs in economically underdeveloped and emerging economies, where it is also common to prepay for many other recurring services, such as utility bills, due to the lack of consumer credit infrastructure.

DOCID: <WO____2004088641A2_I_>

Referring to FIG. 1 and FIG. 2, a prior art method 100 for prepaying for mobile phone services includes the following steps. First, a customer 110 pays a merchant 120 (111) and receives a scratch card 160 in return (112). Scratch card 160 includes a hidden authorization code 180 covered with a protective coating 170. Customer 110 removes the protective coating 170 using a coin or fingernail to reveal the hidden authorization code 180. Authorization code 180 is also referred to as a "hidden recharge number" (HRN) or a "voucher" or a "voucher number". Next, customer 110 contacts a mobile operator 130 and provides the mobile operator 130 with the authorization code 180 through the mobile operator's call center or an interactive voice response system (113). Mobile operator 130 validates the authorization code 180, "recharges" or "tops up" customer's mobile account with the value associated with the authorization code 180, and notifies customer 110 upon completion of the top up transaction (114). The merchant 120 purchases scratch cards in bulk in multiple denominations for multiple mobile operators 130 from either a scratch card distributor 150 (115) or a wholesaler 140 (118). Typically wholesaler 140 purchases mobile airtime minutes in bulk in advance from several mobile operators 130 (117), manufactures the scratch cards 160 and sells the cards either directly to merchants 120 (118) or through a distributor 150 (116). Typically, merchants 120 are convenience stores, department stores or supermarkets that sell many other types of consumer merchandise. In one example, merchant 120 is a Sam's Club and scratch card 160 is an AT&T phone card. Although this is the most widely used method for topping up mobile phone accounts, the costs associated with scratch card manufacturing, distribution, inventory and potential fraud result in reduced profitability for the mobile operator 130. These costs could represent up to 30% of the face value of the scratch card 160. For example for a typical scratch card 160 with a face value amount of $100, the mobile operator only realizes about $70 in revenue due to the above mentioned costs associated with scratch cards.

Dedicated Point of Sale (POS) terminals and Automated Teller Machines (ATMs) are also used to provide a more cost effective way to top up mobile prepaid accounts by electronically generating and printing the voucher at the time of the purchase. Referring to FIG 3, a prior art method 200 for topping up mobile prepaid accounts includes the following steps. First, customer 110 pays merchant 120 (211). Merchant 120 engages a Point of Sale (POS) Terminal 121 to connect over a telecommunication

network 80 to a remote prepaid system 190 (210, 215). Merchant 120 generates a voucher number (not shown) and prints the voucher number onto a receipt 123 using a printer 122 that is in connection with the POS terminal 121. Next, merchant 120 provides the customer 110 with the voucher receipt 123 that contains the voucher number (not shown) (212). Next, customer 110 provides the mobile operator 130 with the voucher number printed on the voucher receipt 123 (213), the mobile operator 130 validates the voucher number and tops up the customer's mobile account with the value associated with the voucher number (214). Mobile operator 130 also notifies customer 110 upon completion of top up transaction (214). These electronic vouchers are created "online" one at a time by the POS terminal 121 by connecting to prepaid system 190 for each customer 110. Alternatively, the POS terminal 121 connects to the prepaid system 190 less frequently, downloads a batch of multiple vouchers that are securely stored within the memory of the POS terminal 121 and subsequently generates the electronic vouchers "offline" for each customer 110. The problem with this prior art method is the fact that there are not many POS or ATMs readily available to accommodate the number of transactions and users. Accordingly, there is a need for a low cost alternative for a mobile POS or ATM that can securely, store, generate, transfer and print electronic prepaid vouchers.

Summary of the Invention

In general, in one aspect of this invention features a system for generating and storing one or more prepaid electronic vouchers in a voucher smart card. The system includes a voucher host system adapted to generate the prepaid electronic vouchers and a voucher terminal adapted to receive the prepaid electronic vouchers from the voucher host system over a network connection and to store the prepaid electronic vouchers in the voucher smart card.

Implementations of this aspect of the invention include the following. The system may further include a transaction server adapted to mediate and aggregate transactions and communications between the voucher terminal and the voucher host system over the network connection. The voucher smart card may be a removable smart card such as a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM)

SDOCID: <WO 2004088641A2 I >

smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card or combinations thereof. The voucher smart card may be a hardware security module (HSM) such as microprocessors or storage accessories. The voucher terminal may be a wireless communication device equipped with a smart card reader/writer module such as a mobile phone, a personal digital assistant (PDA), a pager, a point of sale (POS) terminal, a television remote control, a personal computer or combinations thereof. The smart card reader/writer module is adapted to receive and read/write information stored in/to the voucher smart card, respectively. The voucher terminal may be a wired communication device equipped with a smart card reader/writer module such as a phone, a wired personal digital assistant (PDA), a point of sale (POS) terminal, a television, a personal computer or combinations. The voucher terminal may be a wireless communication device having a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to the SIM card slot and the smart card reader/writer module is adapted to receive and read/write information stored in/to the voucher smart card, respectively. The network may be the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) or a private communication network. The wireless wide area network (WWAN) may be a Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access (CDMA), CDMA 2000, or wideband CDMA (WCDMA). The communications between the voucher host system and the voucher terminal may have a format such as Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), or proprietary message formats. The system may also include a printer adapted to connect to the voucher terminal for printing hard copies of the prepaid electronic vouchers. The printer may be connected to the voucher terminal via a wired connection such as a serial connection, a parallel connection, a Universal Serial Bus (USB) connection or a mini USB connection. Alternatively, the printer may connect to the voucher terminal via a wireless connection such as infrared, Bluetooth, 801.1x, or other short-range radio frequency connections. The prepaid electronic vouchers may have data such as a mobile operator code, a voucher number, a voucher expiration date, the voucher number in an

encrypted format, a voucher value, a voucher currency code, a voucher product code, a voucher product description, a voucher owner code, or a voucher owner. The prepaid electronic vouchers may have encrypted data and the system may further include a voucher encryption smart card that has a voucher encryption key for decrypting the encrypted data. The voucher encryption key may be a personal identification number (PIN), a private key, a public key, a symmetric key or an asymmetric key. The decrypting may utilize techniques such as symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI). The voucher terminal may further include a first voucher application and the first voucher application may provide for retrieving of the stored electronic prepaid vouchers from the voucher smart card and printing hard copies of the prepaid electronic vouchers. The first application may further provide decrypting encrypted data stored in the electronic prepaid vouchers. The voucher terminal may further include a second voucher application and the second voucher application may provide transferring one or more of the stored prepaid electronic vouchers from the voucher smart card to another voucher smart card.

In general in another aspect the invention features a method for generating and distributing one or more prepaid electronic vouchers issued by a merchant for providing a service or a product. The method includes providing a voucher host system adapted to generate the prepaid electronic vouchers and providing a voucher terminal adapted to receive the prepaid electronic vouchers from the voucher host system over a network connection and to store the prepaid electronic vouchers in a voucher smart card. Next, placing a purchase order and paying for one of the one or more prepaid electronic vouchers from the voucher terminal to the voucher host system over the network connection. Next, downloading the one prepaid electronic voucher from the voucher host system to the voucher terminal over the network connection and storing the one prepaid electronic voucher in the voucher smart card. Next, retrieving the one prepaid electronic voucher from the voucher smart card and presenting the one prepaid electronic voucher to the merchant and receiving the service or product.

Implementations of this aspect of the invention include the following. The method may further include printing a hard copy of the one prepaid electronic voucher before presenting the one prepaid electronic voucher to the merchant. The electronic prepaid voucher may have encrypted data and the method may further include decrypting the encrypted data by inserting an encryption smart card in the voucher terminal, retrieving an encryption key and using it to decrypt the encrypted data. The method may further include transferring the one prepaid voucher from the voucher smart card to a second voucher smart card or to a second voucher terminal.

Among the advantages of this invention may be one or more of the following. When compared to the scratch card method the advantages to storing vouchers on a smart card instead of printing the vouchers onto scratch cards are cost and security. Although the cost of a smart card is significantly higher than a paper or plastic scratch card, the smart card can be used thousands of times to store vouchers whereas the scratch card is used once by the customer and then discarded. Vouchers represent monetary value and therefore security is extremely important. Storing encrypted voucher numbers on a smart card is inherently more secure than scratch cards for several reasons. Scratch cards themselves have no "built in" securities features and rely on a secure manufacturing, distribution and sales environment. In the event of theft of a batch of scratch cards, the person in possession of the scratch cards needs only to remove the protective coating on the card to access the voucher number, a breach in security can occur at the merchant location or at any point in the scratch card manufacturing and distribution process. Smart Cards, however, have many "built in" security features that establish a tamper resistant environment for securely storing data from logical and physical attacks which is the primary reason that the financial industry is moving away from magnetic stripe cards to smart cards for debit, credit and electronic cash applications and the primary reason that mobile network operators utilize Subscriber Identity Module (SIM) smart cards. In the event of theft of a smart card with vouchers, the person in possession of the smart card would first have to compromise the security of the smart card to access the encrypted vouchers, then compromise the voucher encryption key that may be stored on the same card or on a different card. The expense and time required to successfully carry out such an attack is significantly more costly than the value of the vouchers on the smart card.

When compared to other Point of Sale (POS) voucher methods, the present invention has the advantage of mobility. The existing prior art POS voucher methods store the vouchers within the device but do not separate storage from fulfillment, i.e., one device is used for both purposes. In the present invention, vouchers are stored on a removable smart card that can be used by one device for voucher storage transactions and then removed and inserted into another device for voucher generation and printing. The present invention provides secure mobility for voucher generation and printing enabling one transaction device to store transactions on a smart card and multiple devices can be deployed to service customer needs remotely.

Brief Description of the Drawings

FIG. 1 is a block diagram of a prior art system for prepaying for mobile phone services;

FIG. 2 is a schematic diagram of a prior art prepaid phone scratch card;

FIG. 3 is schematic diagram of a prior art electronic prepaid voucher system;

FIG. 4 is schematic diagram of an electronic prepaid voucher system that utilizes smart cards according to this invention;

FIG. 5 is a flow diagram of a voucher download transaction to a smart card according to this invention;

FIG. 6 is a flow diagram of a voucher generation transaction from a smart card and print transaction according to this invention;

FIG. 7 is a diagram representing the screen flow and application logic of a mobile transaction terminal application according to this invention;

FIG. 8 is a flow diagram of a voucher transfer transaction according to this invention; and

FIG. 9 is a diagram representing the screen flow and application logic of a voucher transfer transaction according to this invention.

Detailed Description of the Invention

The present invention describes a system and a method for using a transaction terminal for downloading and storing prepaid electronic vouchers on a first smart card, retrieving and decrypting prepaid vouchers from the first smart card and printing a voucher receipt in a printer that is connected with the transaction terminal. The present invention also describes a system and a method for storing a voucher encryption key on a second smart card and then using the second card to decrypt encrypted vouchers on the first smart card. The present invention also describes a system and a method of transferring prepaid vouchers between voucher smart cards.

Referring to FIG. 4, a system 300 for downloading and storing prepaid electronic vouchers on a smart card includes a Prepaid Host System 190, a Mobile Transaction Server 191, a Transaction Terminal 125, a Mobile Transaction Terminal 121, a Printer 122, a Voucher Smart Card 124, a Voucher Encryption Key Smart Card 126, and a Voucher Receipt 123. The Prepaid Host System 190 is the primary source for generating voucher information. The Mobile Transaction Server 191 connects to the Prepaid Host System 190 over telecommunication network 82 and to the transaction terminal 125 and the mobile transaction terminal 121 over telecommunication networks 80, and 81 respectively. Mobile Transaction Server 191 functions as a gateway that mediates and aggregates the transactions between the Prepaid Host System 190 and the transaction terminal 125 and the mobile transaction terminal 121. In one example, Voucher Smart Card 124 and Voucher Encryption Key Smart Card 126 are removable smart cards including "full-size" smart cards, such as credit cards, debit cards, contactless smart cards, stored-value cards, coupon cards, reward cards, electronic cash cards, loyalty cards, identification cards and secure access application or "plug in" format smart cards like those used for Subscriber Identity Modules (SIM's) smart cards utilized by mobile telephones or Secure Access Modules (SAM's) smart cards utilized by Point of Sale (POS) devices. In another example Voucher Smart card 124 and Voucher Encryption Card are hardware security modules (HSM) including accessories that are added to computers, servers and Personal Digital Assistants (PDA's) for banking and secure access applications and secure

BNSDOCID: <WO 2004088641A2 | >

microprocessors that are utilized by Point of Sale (POS) devices. Voucher Encryption Key smart cards have the ability to securely store data and resist tampering and can generate cryptographic keys and encrypt/decrypt data utilizing a cryptographic co-processor. Telecommunications networks 80, 81 and 82 can be the Internet, a public telecommunication network, a private telecommunication network, a local area network (LAN) wireless wide area network (WWAN), a wireless local area network (WLAN) or a personal area network (PAN). The data exchanged using telecommunications networks 80, 81 and 82 have a format such as Short Message Service (SMS), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), or Simple Network Management Protocol (SNMP) over Transmission Control Protocol/Internet Protocol (TCP/IP). Transaction Terminal 125 and Mobile Transaction Terminal 121 are capable of receiving a voucher smart card and printing a voucher receipt 123 via a printer 122 (not shown for Terminal Transaction 125).

Referring to FIG. 10, in one example, the transaction terminal 125 is a mobile phone that is capable of receiving smart cards 902, 903, 904 as described in PCT application WO 99/66752 entitled "Communication Method and Apparatus Improvement", the entire content of which is incorporated herein by reference. In other examples, the transaction terminal 125 is a Point of Sale terminal equipped with a smart card reader, or a Personal Computer (i.e. lap top, desk top, workstation) equipped with a smart card reader or a Personal Digital Assistant (PDA) equipped with a smart card reader. Similarly, the mobile transaction terminal 121 is a mobile phone as shown in FIG. 10 equipped with a smart card reader, or a Personal Computer (i.e. lap top, desk top, workstation) equipped with a smart card reader or a Personal Digital Assistant (PDA) equipped with a smart card reader. In another example, the mobile transaction terminal 121 is a smart card reader equipped with a keypad and a display.

A merchant utilizes the present invention to sell prepaid vouchers to consumers, and the consumers use this invention to recharge their prepaid account. For example, at the beginning of each day, the merchant uses the transaction terminal device described in this invention to connect to a prepaid host system and download a batch of prepaid vouchers in various denominations to a smart card. The merchant may be a small convenient storeowner, a large supermarket sales clerk, an independent sales representative or a sales representative working for a telecommunication company.

:DOCID: <WO 2004088641A2_I_>

Throughout the day the merchant sells the prepaid vouchers to customers who are interested in purchasing a voucher. The customers pay the merchant with cash, credit or debit card. Alternatively, a customer approaches the merchant for purchasing a voucher. The merchant uses the transaction terminal device of this invention to retrieve a voucher from the smart card and prints a receipt for the customer with the voucher number on it. The customer then contacts his service provider and gives the voucher number to the service provider at which point the service provider validates the voucher number and "tops up' or "recharges" the customer's account. The voucher numbers are encrypted on the smart card. The encryption key required to decipher the encrypted information is stored on another smart card. Both cards, i.e., the smart card with the encrypted voucher number and the smart card with the encryption key, need to be present in the transaction terminal device of this invention in order to decrypt, retrieve and present a voucher number for the customer. This process of batch downloading and individual retrieving of vouchers may be distributed among several individuals. For example, a sales manager may download batches of vouchers to multiple smart cards and give each smart card to individual sales representatives. The sales manager may utilize separate smart cards for individual prepaid products, i.e. one card for a mobile operator and another smart card for a long distance telecommunication provider. The sales manager may require the individual sales representatives to pay a deposit or the full amount of value of the vouchers stored on the smart card in advance. Throughout the day, as the sales representatives deplete their inventory the sales manager may also transfer additional vouchers to sales representatives remotely using the transaction terminal device and system described in the present invention. At the end of the day, the sales representatives return their smart cards to the sales manager at which point the sales representatives and the merchant reconcile the financial transactions. Alternatively, the financial settlement may occur remotely and electronically.

Referring to FIG. 5, the process of downloading a voucher includes the following steps. First, the transaction terminal 125 establishes a connection with the mobile transaction server 190 over network 80 (410). Next, mobile transaction server 191 routes the transaction request to the prepaid host system 190 through network 82 (411). The prepaid host system 190 validates the connection and transmits a specified

BNSDOCID: <WO 2004088641A2 | >

quantity and types of vouchers to the mobile transaction server 191 over network 82 (412). The mobile transaction server 191 routes the downloaded vouchers to the transaction terminal 125 through network connection 80 (413). In one example, the data in the voucher download transaction for a single voucher include, a code representing the mobile operator that the voucher is associate with, a voucher serial number, a voucher expatriation date, the voucher number in its encrypted format, the voucher value and a code representing the currency of the voucher value. Upon completion of the voucher download transaction, the transaction terminal 125 transmits a transaction complete acknowledgement to the mobile transaction server 191 through network connection 80 (416) and the mobile transaction server 191 transmits this acknowledgement to the prepaid host system 190 over network 82 (417). The transaction terminal 125 is in connection with a voucher smart card 124 and sends the voucher data to the voucher smart card 124 (414). Upon completion of the transaction the transaction terminal 125 receives an acknowledgement from the voucher smart card 124 (415). In one embodiment, the Prepaid Host System 190 determines the quantity and types of vouchers that are downloaded to the Transaction Terminal 125. In this embodiment the connection is initiated by the prepaid host system 190 (408, 409). In another embodiment, the Transaction Terminal 125 determines the quantity and types of vouchers that are downloaded to the Transaction Terminal 125.

Referring to FIG. 6 and FIG. 7, a method 500 for retrieving a voucher from a smart card 124 and printing a voucher receipt 124 includes the following steps. First, a user utilizes a mobile transaction application 600 stored on the mobile transaction terminal 121 to start a new transaction (610). The user is then prompted to insert the voucher smart card 124 into the mobile transaction terminal 121 (612). The mobile transaction application 600 on the mobile transaction terminal 121 accesses the voucher smart card 124 (517) and retrieves the inventory of available vouchers (518). The inventory of available mobile operators is displayed on the mobile transaction terminal application and the user is prompted to make a selection (614). Following the selection of a specific mobile operator, the inventory of available voucher values for the selected mobile operator is displayed and the user is prompted to make a selection (616). Following the selection of a specific voucher, the user is prompted to confirm the selection (618). Upon confirmation, the mobile transaction application

3DOCID: <WO 2004088641A2_I_>

600 accesses voucher smart card 124 (519), retrieves the voucher data associated with the confirmed selection (520), updates the inventory on the voucher smart card 124 (521) and stores the voucher data within the memory (not shown) of the mobile transaction terminal 121. Next, the mobile transaction application 600 accesses the voucher encryption key smart card 126 (510), and if the mobile transaction terminal 121 is not in connection with the voucher encryption key smart card 126, the user is prompted to insert the voucher encryption key smart card 126 (620). The mobile transaction application 600 accesses the voucher encryption key smart card 126 to retrieve smart card profile information (511). If the mobile transaction terminal 121 is configured to receive only one smart card, the user is asked to remove the voucher smart card 124 and replace it with the voucher encryption key smart card 126. In one example, the voucher encryption key smart card 126 is protected from unauthorized access with a Personal Identification Number (PIN) and the user is prompted to enter a valid PIN (622). The users types the PIN and the mobile transaction application 600 presents the PIN to the voucher encryption key smart card 126 (512) for authorization. The authorization result is returned to the mobile transaction application 600 (513) and upon successful authorization, the mobile transaction application 600 retrieves the voucher encryption key (not shown) (514). The voucher encryption key is utilized by the mobile transaction application 600 to decrypt the encrypted voucher information that was previously retrieved by the mobile transaction application 600 from the voucher smart card 124. The decryption process (not shown) utilizes symmetric keys or asymmetric keys and cryptographic techniques such as Data Encryption Standard (DES, 3DES), RSA, Elliptical Curve Cryptography (ECC), Message Authentication Codes (MAC, HMAC), SHA-1, AES and Public Key Infrastructure (PKI). When the voucher decryption is completed, the user is prompted to either print or view the decrypted voucher information on the screen (626). The mobile transaction terminal 121 is in connection with a printer 122. Communication 70 with the printer 122 is either wired (i.e. serial, parallel, USB) or wireless (i.e. infrared, Bluetooth, 802.1x). If the user selects the print option, the mobile transaction terminal 121 establishes connection 70 with the printer 122 and sends the voucher data to the printer (522). The printer 122 formats the voucher data accordingly, generates voucher receipt 123 (524) and acknowledges results of print process to the mobile transaction terminal 121 (523). Alternatively, the user selects to present the voucher data on the display (not shown) of the mobile transaction terminal

BNSDOCID: <WO 2004088641A2 | >

121. The mobile transaction application 600 reestablishes connection with the voucher smart card 124 to update the voucher inventory with the completed transaction details (525). Once a voucher is retrieved, the voucher is either deleted from the inventory or its status is changed such that it can no longer be retrieved.

The present invention also defines a process for transferring vouchers between voucher smart cards. In one case, the voucher transfer process is local and it uses the same transaction terminal (mobile or otherwise) to transfer vouchers from one voucher smart card to another voucher smart card. In another case the voucher transfer process is remote and it uses one transaction terminal (mobile or otherwise) to transmit voucher data to another transaction terminal (mobile or otherwise). Referring to FIG. 8 and FIG. 9, using voucher transfer application 800, a user initiates a voucher transfer transaction 700. The user is prompted to insert the origin voucher smart card 124 that stores the vouchers into the transaction terminal 125. The voucher transfer application 800 accesses voucher smart card 124 (717) and retrieves the inventory of available vouchers (718). The inventory of available mobile operators is displayed on the transaction terminal application and the user is prompted to make a selection (814). Following the selection of a mobile operator, the inventory of available voucher values for the selected mobile operator is displayed and the user is prompted to make a selection (816). Following the selection of a voucher value, the inventory of available vouchers for the selected operator and value denominations are displayed and the user is prompted to select a quantity of vouchers that is less than or equal to the total quantity of vouchers available (818). Following the selection of one or more vouchers, the use is prompted to confirm the selection (819). Upon confirmation, the voucher transfer application 800 accesses voucher smart card 124 (719), retrieves the voucher data associated with the confirmed selection (720), updates the inventory on the voucher smart card 124 and stores the voucher data within the memory (not shown) of the transaction terminal 125 (721). In one example, the transfer of vouchers requires authorization. If the transaction terminal 125 is configured to receive only one smart card, the user is required to remove the voucher smart card 124 and replace it with the voucher encryption key smart card 126. In one example, the voucher encryption key smart card 126 is protected from unauthorized access with a Personal Identification Number (PIN) and the user is prompted to enter a valid PIN (822). The users types the PIN, the voucher transfer

application 800 presents the PIN to the voucher encryption key smart card 126 for authorization (712) and the authorization result is returned to the voucher transfer application 800 (713). Upon successful authorization, the voucher data are transferred from the memory (not shown) of the transaction terminal 125 to a temporary storage repository on the voucher encryption key smart card 126 (714) and then the user is prompted to choose the transfer method (824). The transfer method is either a local "card to card" transfer or a remote transfer. If the user selects the local "card to card" transfer option, the user is prompted to insert the destination voucher smart card 124a (828). The voucher transfer application 800 retrieves the voucher data from the temporary storage repository on the voucher encryption key smart card 126 (715) and appends the voucher data to the destination voucher smart card 124a (722). After receiving the voucher data, the destination voucher smart card 124a provides an acknowledgement response to the transaction terminal application (723) that is further routed to the voucher encryption key smart card 126 to complete the card transfer transaction (716). If the transaction terminal is configured to receive only one smart card, the user is prompted to remove and insert the origin voucher smart card 124, the voucher encryption key smart card 126 and the destination voucher smart card 124a in the appropriate sequence to complete the transaction (830). If the user selects the remote transfer option, the user is prompted to enter the Identification Number of the destination transaction terminal (826). The voucher transfer application 800 transmits the voucher data to the mobile transaction server 191 over network 80 (724). Mobile transaction server 191 transmits an acknowledgment of the receipt of the voucher data over network 80 to transaction terminal 125 which is then routed to the voucher encryption key smart card 126 to complete the transaction from the origin of the transfer (716). The mobile transaction server 191 transmits a notification to the mobile transaction terminal 121 designated by the origin 826 over network 81 (726). The mobile transaction terminal 121 receives the notification (726) and transmits an acknowledgement and a download request from the mobile transaction server 191 over network 81 (727). The mobile transaction server 191 transmits the voucher download to mobile transaction terminal 121 over network 81 (728). The user is prompted to insert the voucher smart card 124b and a voucher transaction application 800a on the mobile transaction terminal 121 appends the voucher data to the destination voucher smart card 124b (729). A voucher data transfer acknowledgement is transmitted to the mobile transaction

terminal 121(730) and routed to the mobile transaction server 191 over network 81 to complete the remote transfer transaction (731).

In another embodiment, the transaction terminal (mobile or otherwise) is also a payment terminal that enables the user to accept and process electronic payments as described in a co-pending patent application entitled "System and method for payment transaction authentication", the entire content of which is incorporated herein by reference. In another embodiment, the transaction terminal (mobile or otherwise) is also configured to receive magnetic stripe payment cards as described in a co-pending patent application entitled "Mobile Communication Device Equipped with a Magnetic stripe Reader". In another embodiment, the mobile transaction terminal 121 has no connection to the mobile transaction server. The voucher encryption key smart card 126 and the voucher smart card 124 1 store all transaction information that is transferred to another transaction terminal utilizing the "card to card" transfer method described in FIG. 8 and FIG. 9. In another embodiment, the Prepaid Host System 190 is any type of service that utilizes vouchers such as utilities, local phone service, long distance phone service, pay-per-view entertainment, electronic ticketing. In another embodiment, the encrypted vouchers are stored in the memory of the mobile transaction terminal 121 or transaction terminal 125. The memory is either internal to the mobile device or external and in connection with the mobile device (i.e. Compact Flash, Secure Digital, USB Flash memory, external hard drive). In yet another embodiment, the encrypted vouchers are stored in the memory 901 of the mobile phone attachment as described in PCT application WO 99/66752 entitled "Communication Method and Apparatus Improvement", shown in FIG. 10. Referring to FIG. 4, in another embodiment the mobile transaction terminal 121 has no network connection 81 with the mobile transaction server 191 and is a non-network connected device with the ability to interact with voucher encryption key smart card 126, voucher smart card 124 and optionally voucher printer 122.

Several embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

3DOCID: <WO 2004088641A2_I_>

1. A system for generating and storing one or more prepaid electronic vouchers comprising:

a voucher host system adapted to generate said prepaid electronic vouchers;

a voucher smart card; and

a voucher terminal adapted to receive said prepaid electronic vouchers from said voucher host system over a network connection and to store said prepaid electronic vouchers in said voucher smart card.

2. The system of claim 1 further comprising a transaction server adapted to mediate and aggregate transactions and communications between said voucher terminal and said voucher host system over said network connection.

3. The system of claim 1 wherein said voucher smart card comprises a removable smart card selected from a group consisting of a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM) smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

4. The system of claim 1 wherein said voucher smart card comprises a hardware security module (HSM) selected from a group consisting of microprocessors and storage accessories.

5. The system of claim 1 wherein said voucher terminal comprises a wireless communication device equipped with a smart card reader/writer module selected from a group consisting of a mobile phone, a personal digital assistant (PDA), a pager, a point of sale (POS) terminal, a television remote control, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

BNSDOCID: <WO 2004088641A2 (>

6. The system of claim 1 wherein said voucher terminal comprises a wired communication device equipped with a smart card reader/writer module selected from a group consisting of a phone, a wired personal digital assistant (PDA), a point of sale(POS) terminal, a television, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

7. The system of claim 1 wherein said voucher terminal comprises a wireless communication device comprising a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to said SIM card slot and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

8. The system of claim 1 wherein said network is selected from a group consisting of the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

9. The system of claim 8 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

10. The system of claim 2 wherein said communications comprise a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

11. The system of claim 1 further comprising a printer adapted to connect to said voucher terminal for printing hard copies of said prepaid electronic vouchers.

12. The system of claim 11 wherein said printer is connected to said voucher terminal via a wired connection selected from a group consisting of a serial connection, a parallel connection, a USB connection and a mini USB connection.

13. The system of claim 11 wherein said printer is connected to said voucher terminal via a wireless connection selected from a group consisting of infrared, Bluetooth, 801.1x, and short-range radio frequency (RF) connections.

14. The system of claim 1 wherein said prepaid electronic vouchers comprise data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

15. The system of claim 1 wherein said prepaid electronic vouchers comprise encrypted data.

16. The system of claim 15 further comprising a voucher encryption smart card wherein said voucher encryption smart card comprises a voucher encryption key for decrypting said encrypted data.

17. The system of claim 16 wherein said voucher encryption key is selected from a group consisting of a personal identification number (PIN), a private key, a public key, a symmetric key and an asymmetric key.

18. The system of claim 16 wherein said decrypting utilizes techniques selected from a group consisting of symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI).

19. The system of claim 1 wherein said voucher terminal further comprises a first voucher application wherein said first voucher application provides retrieving of said

stored electronic prepaid vouchers from said voucher smart card and printing hard copies of said prepaid electronic vouchers.

20. The system of claim 19 wherein said first application further provides decrypting encrypted data stored in said electronic prepaid vouchers.

21. The system of claim 1 wherein said voucher terminal further comprises a second voucher application wherein said second voucher application provides transferring one or more of said stored prepaid electronic vouchers from said voucher smart card to another voucher smart card.

22. A method for generating and distributing one or more prepaid electronic vouchers issued by a merchant for providing a service or a product, said method comprising:

providing a voucher host system adapted to generate said prepaid electronic vouchers;

providing a voucher terminal adapted to receive said prepaid electronic vouchers from said voucher host system over a network connection and to store said prepaid electronic vouchers in a voucher smart card;

placing a purchase order and paying for one of said one or more prepaid electronic vouchers from said voucher terminal to said voucher host system over said network connection;

downloading said one prepaid electronic voucher from said voucher host system to said voucher terminal over said network connection and storing said one prepaid electronic voucher in said voucher smart card;

retrieving said one prepaid electronic voucher from said voucher smart card; and

presenting said one prepaid electronic voucher to said merchant and receiving said service or product.

23. The method of claim 22 further comprising providing a transaction server adapted to mediate and aggregate transactions and communications between said voucher terminal and said voucher host system over said network connection.

SDOCID: <WO 2004088641A2 I >

24. The method of claim 22 further comprising printing a hard copy of said one prepaid electronic voucher before presenting said one prepaid electronic voucher to said merchant.

25. The method of claim 22 wherein said one electronic prepaid voucher comprises data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

26. The method of claim 22 wherein said one prepaid electronic voucher comprises encrypted data.

27. The method of claim 26 wherein an encryption key for said encrypted data is stored in an encryption smart card.

28. The method of claim 27 further comprising decrypting said encrypted data by inserting said encryption smart card in said voucher terminal, retrieving said encryption key and using it to decrypt said encrypted data.

29. The method of claim 22 wherein said voucher smart card comprises a removable smart card selected from a group consisting of a "full size" smart credit card, a "full size" smart debit card, a "plug-in" Subscriber Identification Module (SIM) smart card, a "plug-in" Secure Access Module (SAM) smart card, a contactless smart card, a stored-value card, a coupon card, a reward card, an electronic cash card, a loyalty card, an identification card and combinations thereof.

30. The method of claim 22 wherein said voucher smart card comprises a hardware security module (HSM) selected from a group consisting of microprocessors and storage accessories.

31. The method of claim 22 wherein said voucher terminal comprises a wireless communication device equipped with a smart card reader/writer module selected from a group consisting of a mobile phone, a personal digital assistant (PDA), a

pager, a point of sale (POS) terminal, a television remote control, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

32. The method of claim 22 wherein said voucher terminal comprises a wired communication device equipped with a smart card reader/writer module selected from a group consisting of a phone, a wired personal digital assistant (PDA), a point of sale(POS) terminal, a television, a personal computer and combinations thereof, and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

33. The method of claim 22 wherein said voucher terminal comprises a wireless communication device comprising a subscriber identification module (SIM) card slot, a smart card reader/writer module electrically connected to said SIM card slot and wherein said smart card reader/writer module is adapted to receive and read/write information stored in/to said voucher smart card, respectively.

34. The method of claim 22 wherein said network is selected from a group consisting of the Internet, a telecommunications network, a wireless wide area network (WWAN), a wireless local area network (WLAN), a personal area network (PAN) and a private communication network.

35. The method of claim 34 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), General Packet Radio Service (GPRS), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

36. The method of claim 23 wherein said communications comprise a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

37. The method of claim 22 wherein said prepaid electronic vouchers comprise data selected from a group consisting of a mobile operator code, a voucher number, a voucher expiration date, said voucher number in an encrypted format, a voucher value, voucher currency code, voucher product code, voucher product description, voucher owner code, and voucher owner.

38. The method of claim 27 wherein said voucher encryption key is selected from a group consisting of a personal identification number (PIN), a private key, a public key, a symmetric key, and an asymmetric key.

39. The method of claim 28 wherein said decrypting utilizes techniques selected from a group consisting of symmetric keys, asymmetric keys, data encryption standard (DES, 3DES), RSA, elliptical curve cryptography (ECC), message authentication codes (MAC, HMAC, SHA-1, AES, and public key infrastructure (PKI).

40. The method of claim 22 wherein said voucher terminal further comprises a first voucher application wherein said first voucher application provides said retrieving of said stored electronic prepaid vouchers from said voucher smart card and printing hard copies of said prepaid electronic vouchers.

41. The method of claim 40 wherein said first application further provides decrypting of encrypted data stored in said electronic prepaid vouchers.

42. The method of claim 40 wherein said voucher terminal further comprises a second voucher application wherein said second voucher application provides transferring one or more of said stored prepaid electronic vouchers from said voucher smart card to another voucher smart card.

43. The method of claim 22 further comprising transferring said one prepaid voucher from said voucher smart card to a second voucher smart card.

44. The method of claim 22 further comprising transferring said one prepaid voucher from said voucher smart card to a second voucher terminal.

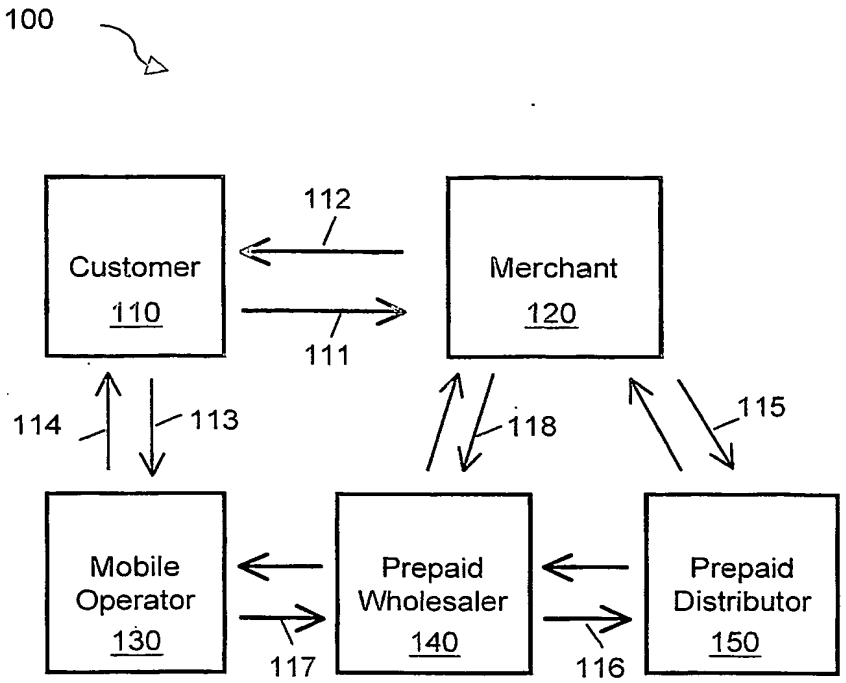


FIG. 1
(Prior Art)

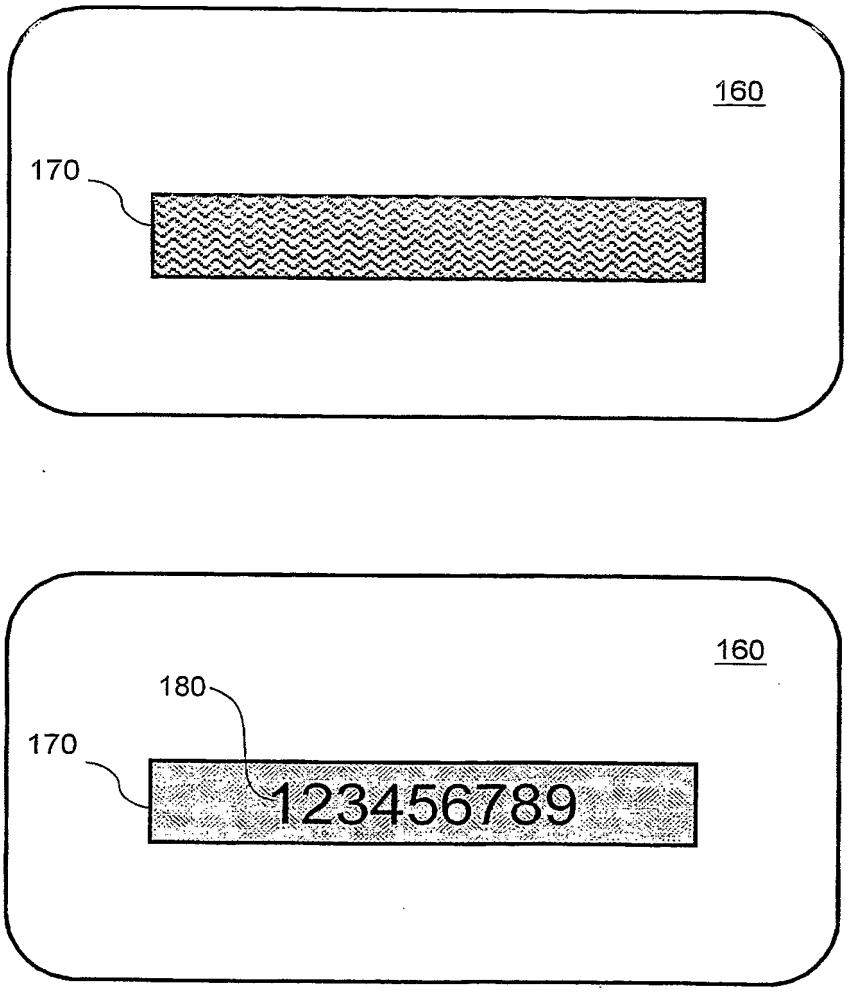


FIG. 2
(Prior Art)

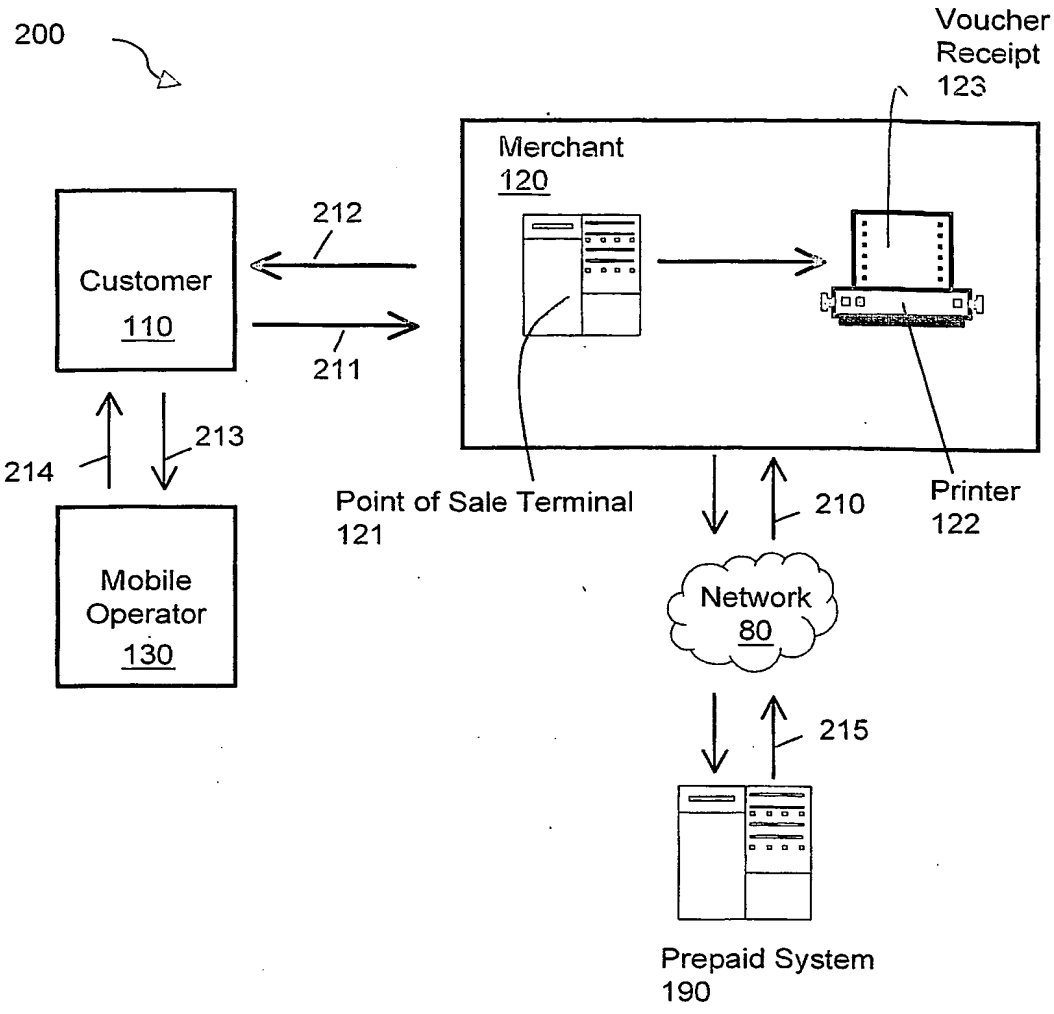


FIG. 3
(Prior Art)

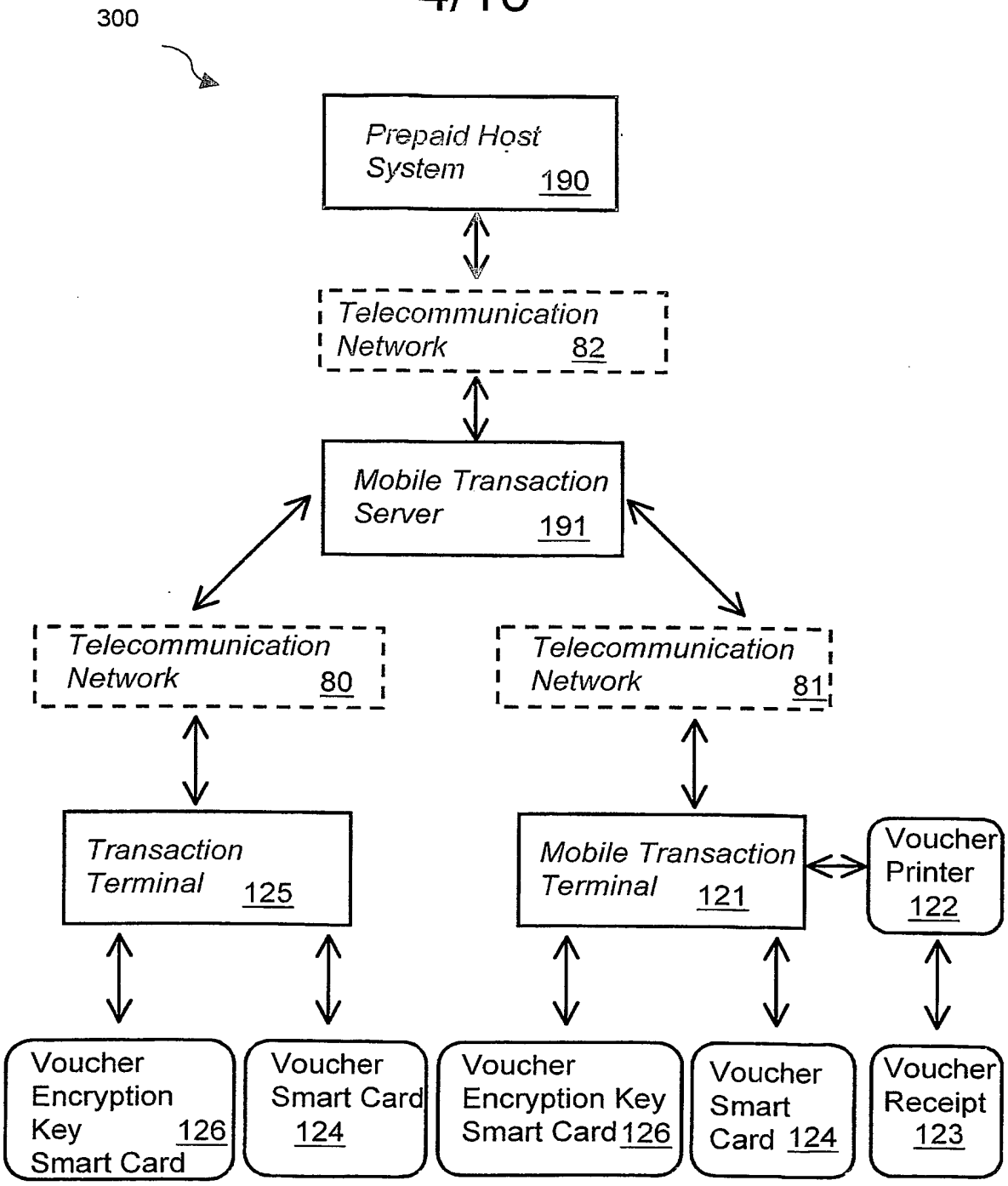

300
Prepaid Host System 190
Telecommunication Network 82
Mobile Transaction Server 191
Telecommunication Network 80
Telecommunication Network 81
Transaction Terminal 125
Mobile Transaction Terminal 121
Voucher Printer 122
Voucher Encryption Key Smart Card 126
Voucher Smart Card 124
Voucher Encryption Key Smart Card 126
Voucher Smart Card 124
Voucher Receipt 123

FIG. 4

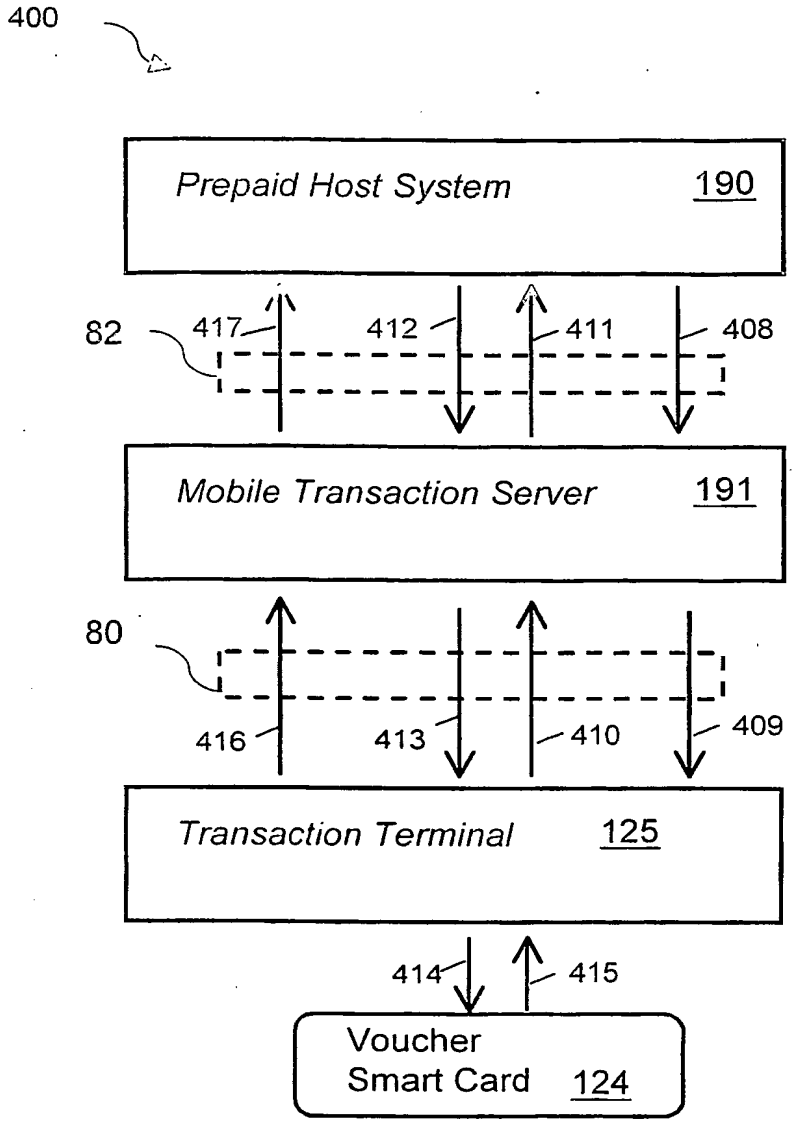

400
Prepaid Host System 190
82
417
412
411
408
Mobile Transaction Server 191
80
416
413
410
409
Transaction Terminal 125
414
415
Voucher
Smart Card 124

FIG. 5

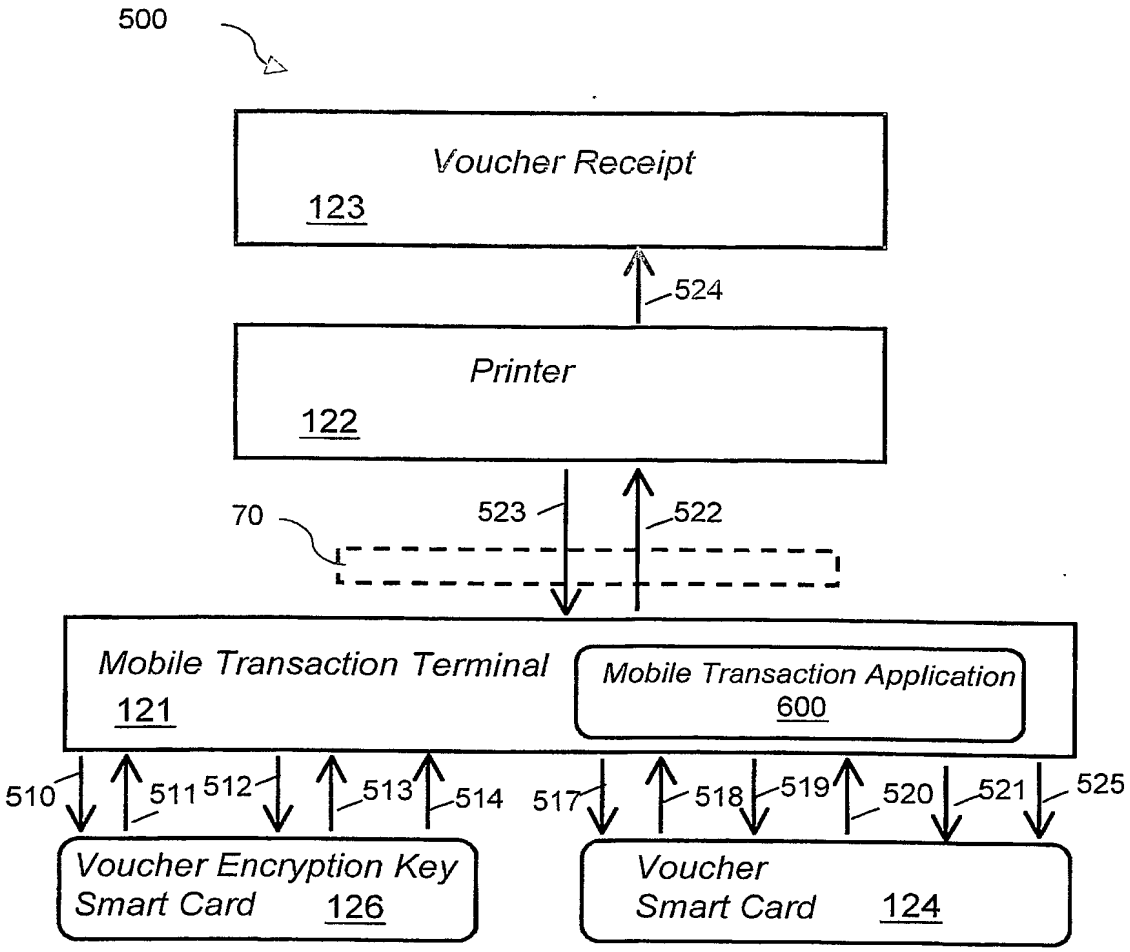

500
Voucher Receipt
123
524
Printer
122
70
523
522
Mobile Transaction Terminal
121
Mobile Transaction Application
600
510
511
512
513
514
517
518
519
520
521
525
Voucher Encryption Key
Smart Card
126
Voucher
Smart Card
124

FIG. 6

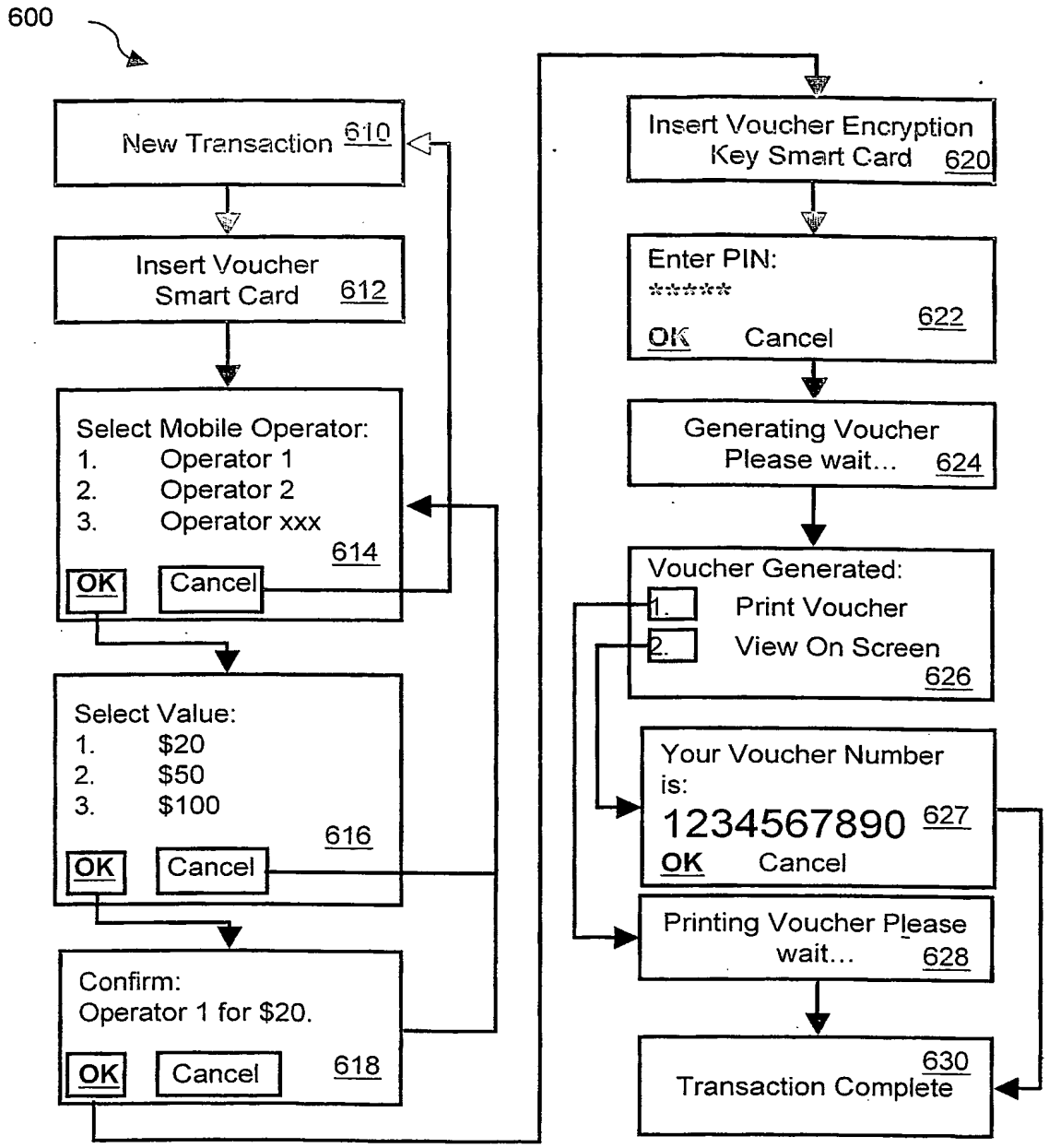

600
New Transaction 610
Insert Voucher Smart Card 612
Select Mobile Operator:
1. Operator 1
2. Operator 2
3. Operator xxx
614
OK
Cancel
Select Value:
1. $20
2. $50
3. $100
616
OK
Cancel
Confirm:
Operator 1 for $20.
OK
Cancel
618
Insert Voucher Encryption Key Smart Card 620
Enter PIN:
*****
622
OK
Cancel
Generating Voucher Please wait... 624
Voucher Generated:
1. Print Voucher
2. View On Screen
626
Your Voucher Number is:
1234567890 627
OK
Cancel
Printing Voucher Please wait... 628
630
Transaction Complete

FIG. 7

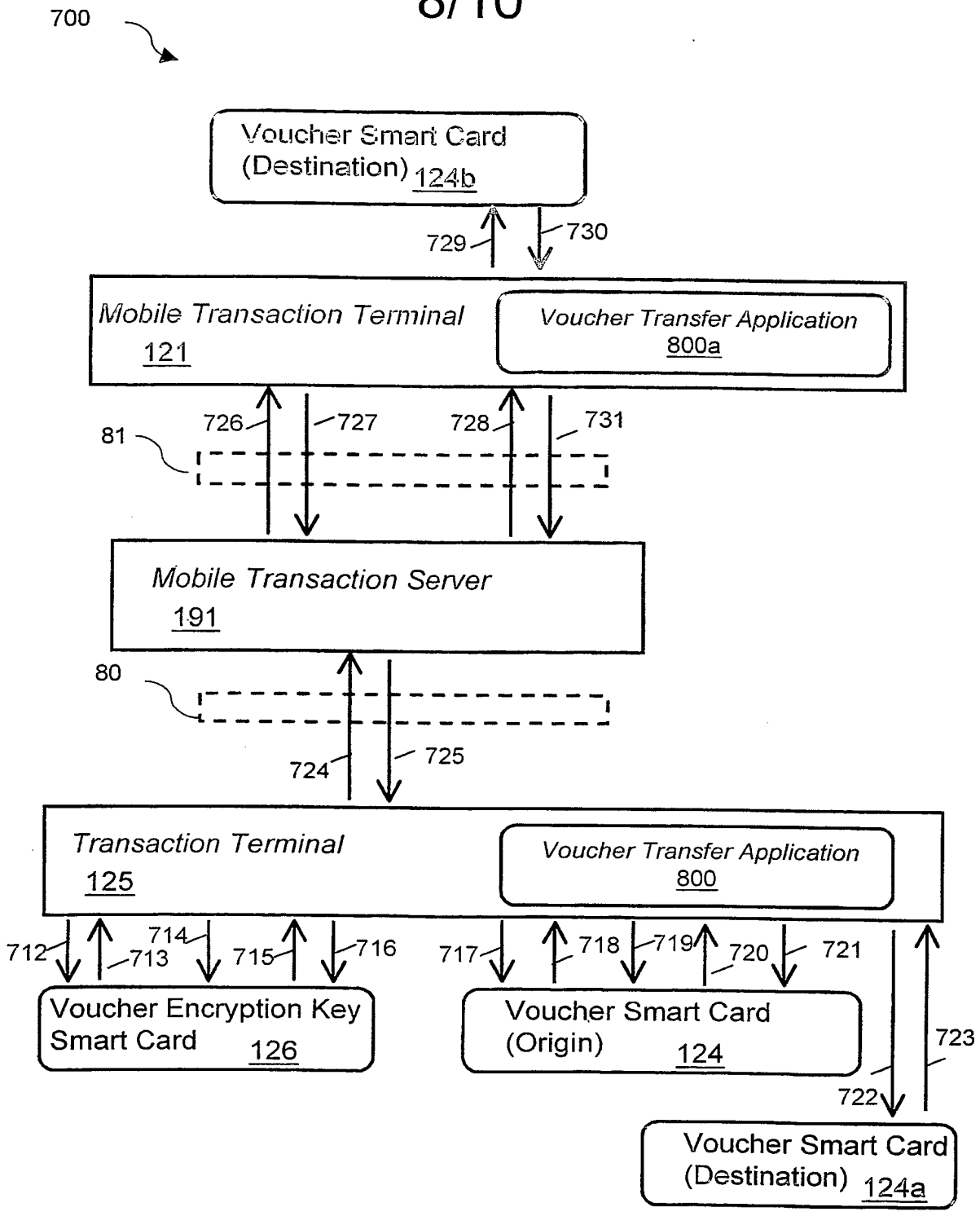

700
Voucher Smart Card (Destination) 124b
729
730
Mobile Transaction Terminal 121
Voucher Transfer Application 800a
81
726
727
728
731
Mobile Transaction Server 191
80
724
725
Transaction Terminal 125
Voucher Transfer Application 800
712
713
714
715
716
717
718
719
720
721
Voucher Encryption Key Smart Card 126
Voucher Smart Card (Origin) 124
723
722
Voucher Smart Card (Destination) 124a

FIG. 8

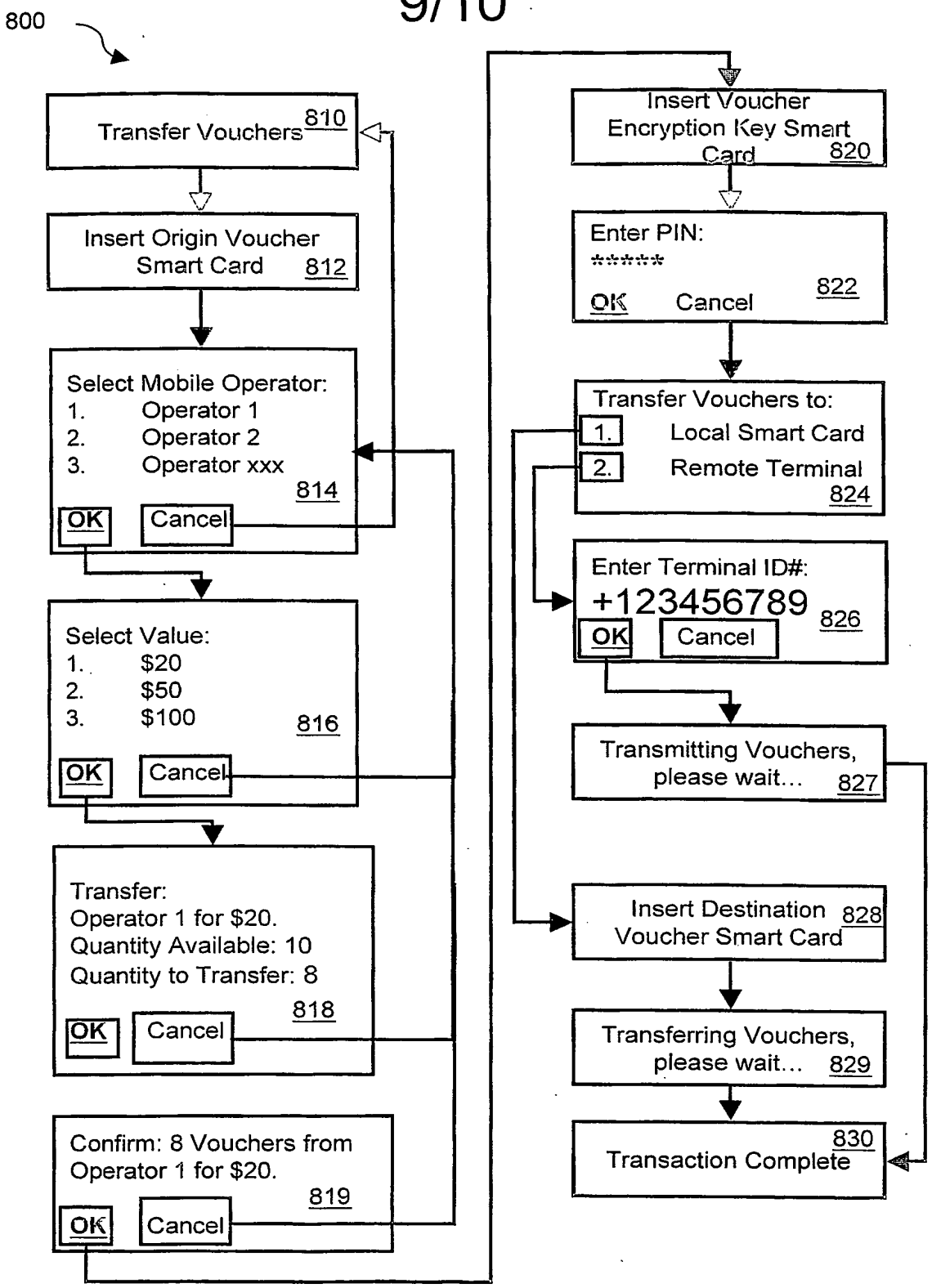

800
Transfer Vouchers 810
Insert Origin Voucher Smart Card 812
Select Mobile Operator:
1. Operator 1
2. Operator 2
3. Operator xxx
814
OK
Cancel
Select Value:
1. $20
2. $50
3. $100
816
OK
Cancel
Transfer:
Operator 1 for $20.
Quantity Available: 10
Quantity to Transfer: 8
818
OK
Cancel
Confirm: 8 Vouchers from Operator 1 for $20.
819
OK
Cancel
Insert Voucher Encryption Key Smart Card 820
Enter PIN:
*****
OK Cancel
822
Transfer Vouchers to:
1. Local Smart Card
2. Remote Terminal
824
Enter Terminal ID#:
+123456789
826
OK
Cancel
Transmitting Vouchers, please wait... 827
Insert Destination Voucher Smart Card 828
Transferring Vouchers, please wait... 829
830
Transaction Complete

FIG.9

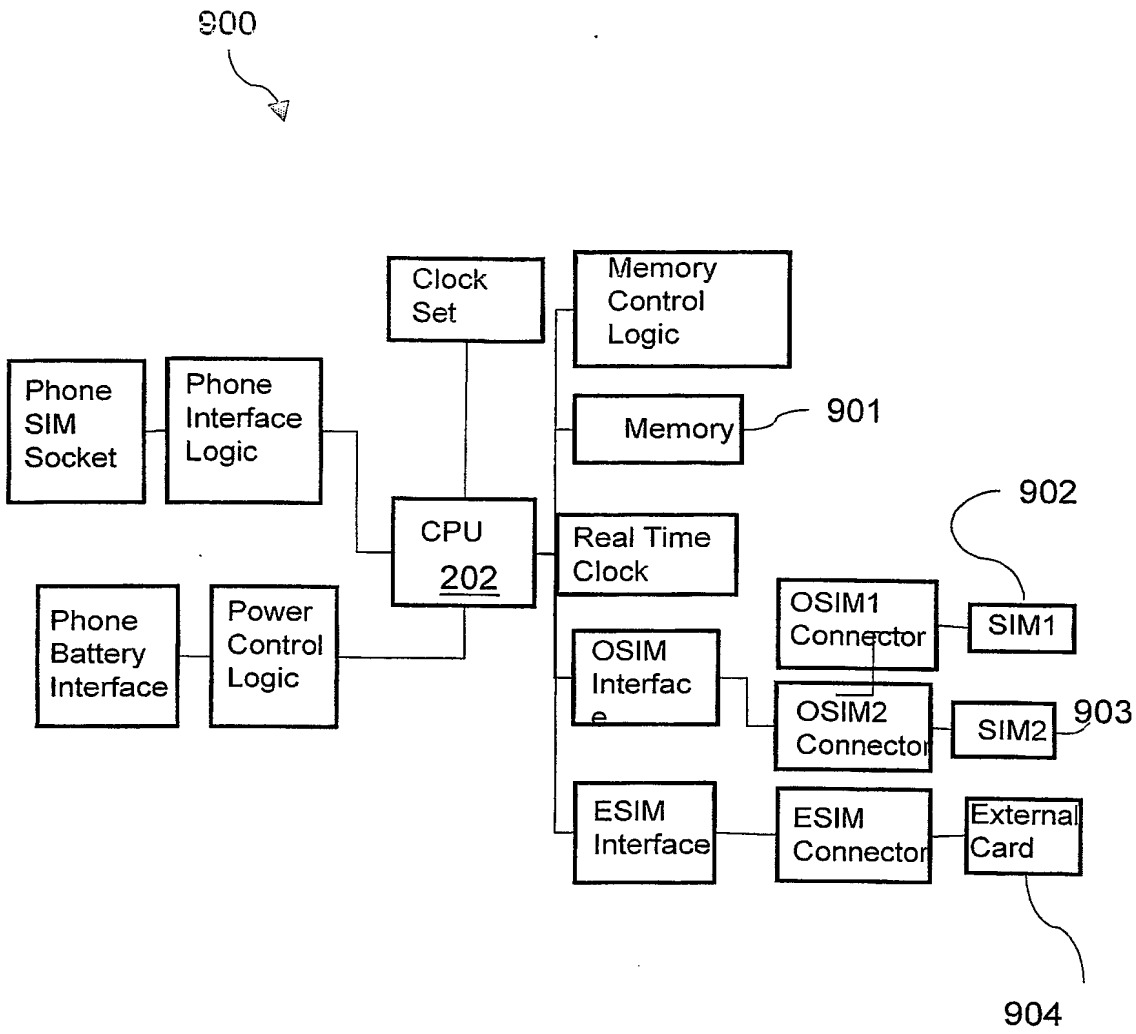

900
Clock Set
Memory Control Logic
Phone SIM Socket
Phone Interface Logic
Memory
901
902
CPU 202
Real Time Clock
Phone Battery Interface
Power Control Logic
OSIM1 Connector
SIM1
OSIM Interfac e
OSIM2 Connector
SIM2
903
ESIM Interface
ESIM Connector
External Card
904

FIG. 10

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number
WO 2004/088641 A2

(51) International Patent Classification[7]: G11B

(21) International Application Number:
PCT/US2004/009149

(22) International Filing Date: 25 March 2004 (25.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/457,716	26 March 2003 (26.03.2003)	US
10/808,697	25 March 2004 (25.03.2004)	US

(71) Applicant *(for all designated States except US)*: **WAY SYSTEMS, INC.** [US/US]; 200 Unicorn Park, Woburn, MA 01801 (US).

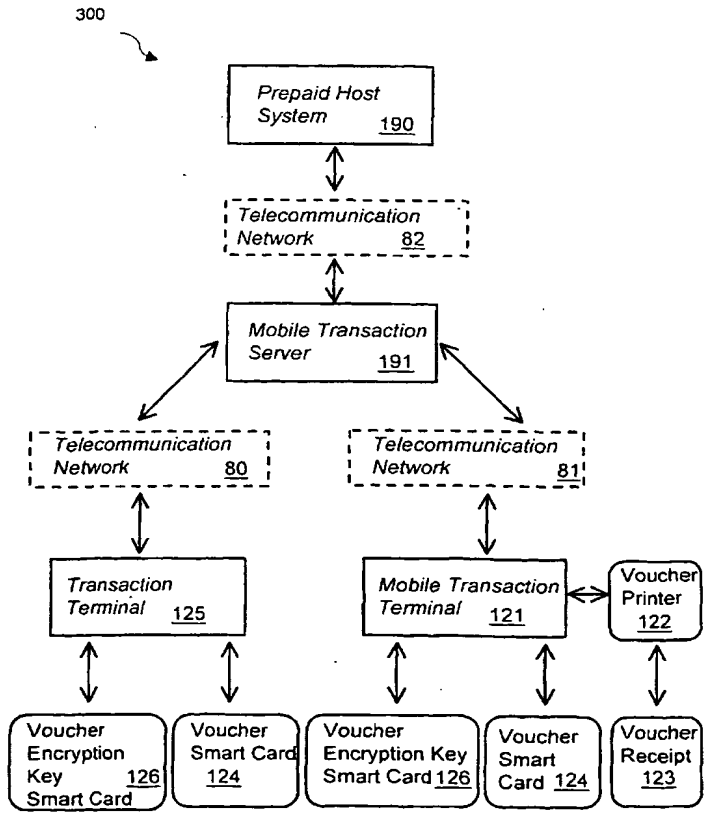
(71) Applicants and
(72) Inventors: **GOLDTHWAITE, Scott** [US/US]; 15 Oregon Court, Hingham, MA 02043 (US). **BALSAN, Damien** [US/US]; 78 Melrose Street, Arlington, MA 02474 (US).

(74) Agent: **COLLINS, Aliki, K.. ph. d.**; AKC Patents, 215 Grove Street, Newton, MA 02466 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURELY STORING, GENERATING, TRANSFERRING AND PRINTING ELECTRONIC PREPAID VOUCHERS



(57) Abstract: The present invention describes a system and a method that utilizes transaction terminals (125, 121) equipped with smart card readers to download and store a batch of multiple prepaid electronic vouchers to a smart card (124), retrieve and decrypt individual prepaid vouchers from the smart card and print a voucher receipt with a printer (122) in connection with the transaction terminal. The transaction terminals (125, 121) are in connection with a mobile transaction server (191) that acts as a gateway to a prepaid system (190) and routes transactions between transaction terminals and the prepaid system and between transaction terminals. The present invention also describes a method for storing a voucher encryption key on a second smart card or hardware security module. The voucher encryption key is utilized to decrypt encrypted vouchers on a voucher repository smart card. The present invention also describes a method of transferring encrypted vouchers between voucher smart cards using a single transaction terminal or multiple transaction terminals. The transaction terminals may be mobile devices communicating to the mobile transaction server over wireless networks or computers connected to a wired network.

WO 2004/088641 A2

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *without international search report and to be republished upon receipt of that report*

(48) Date of publication of this corrected version:
9 December 2004

(15) Information about Correction:
see PCT Gazette No. 50/2004 of 9 December 2004, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ORIGINAL
NO MARGINALIA

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)